# Current Trends in the Threat to Computers:

## From Simple Hacking to Cyber Terrorism

November 12, 1998

Doug L. Mansur, Program Manager
Computer Security Technology Center
Lawrence Livermore National Laboratory

UCRL-MI-132299

**This work was performed under the auspices of the U.S. Dept. of Energy at LLNL under contract no. W-7405-Eng-48**

# *Today's Presentation*

- Highlights of reports form US computer incident response teams
- Changing trends in computer and network attacks
- Emerging new types of attackers
- Attacks: How hard is it?
- Proactive defenses
- Resources available to help

# *Information Assurance Portfolio*

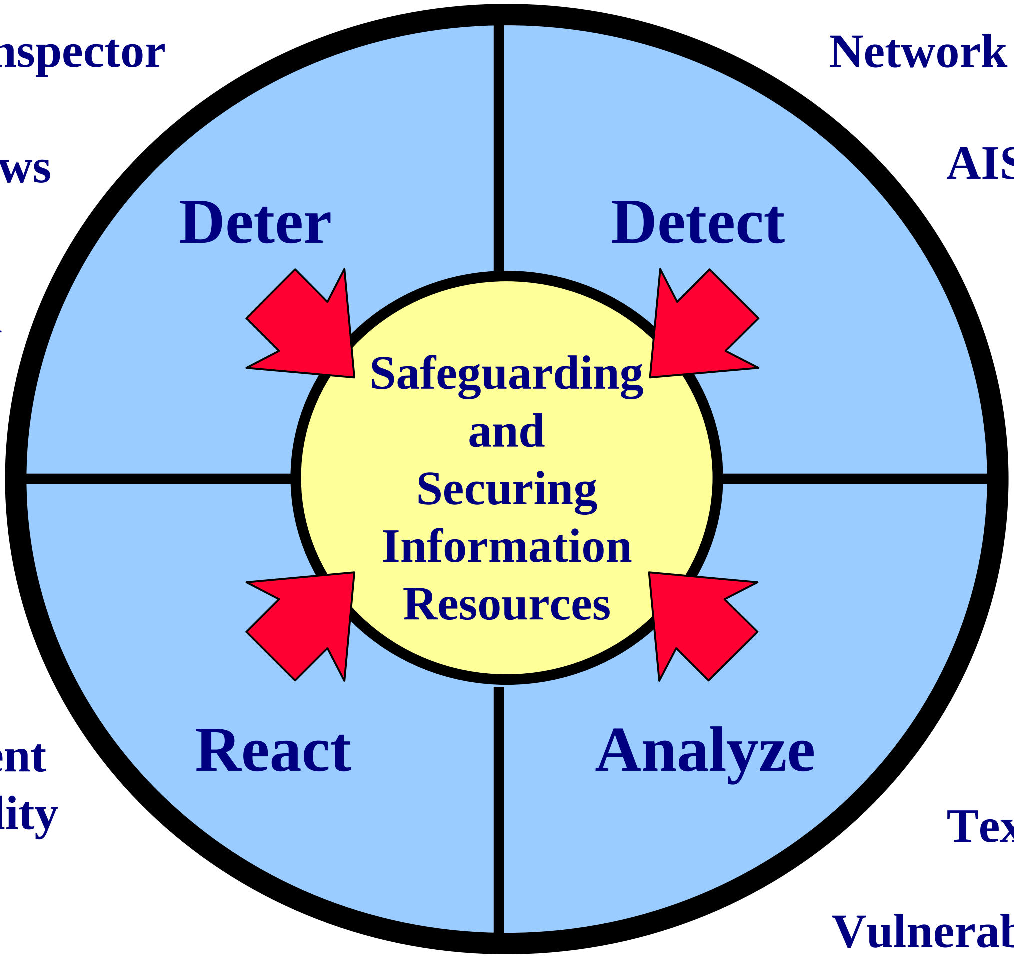
Security Profile Inspector

*"White Hat"* Reviews

Secure Software
Distribution System

Secure Systems
Services

Computer Incident
Advisory Capability



Network Intrusion Detector

AIS Alarms

UnAuTH

Simulation &
Modeling

National INFOSEC
Technical Baseline

DOE-IS Server

Text Analysis Project

Vulnerability Analysis Project

# *Rate of Incidents: DOE/CIAC*

| | FY97 | FY98 |
|---|---|---|
| Number of intrusions | 42 | 123 |
| Number of attempted intrusions | 27 | 355 |
| Number of scans/probes | * | 796 |
| Number involving multiple DOE sites | 8 | 40 |
| Number of virus incidents | 43 | 21 |
| Total number of incidents | **169** | **1335** |

* not tracked

# *Rate of Incidents: CERT/CC*

- **CERT®/CC Statistics 1988-1998**
  **Incidents Reported**

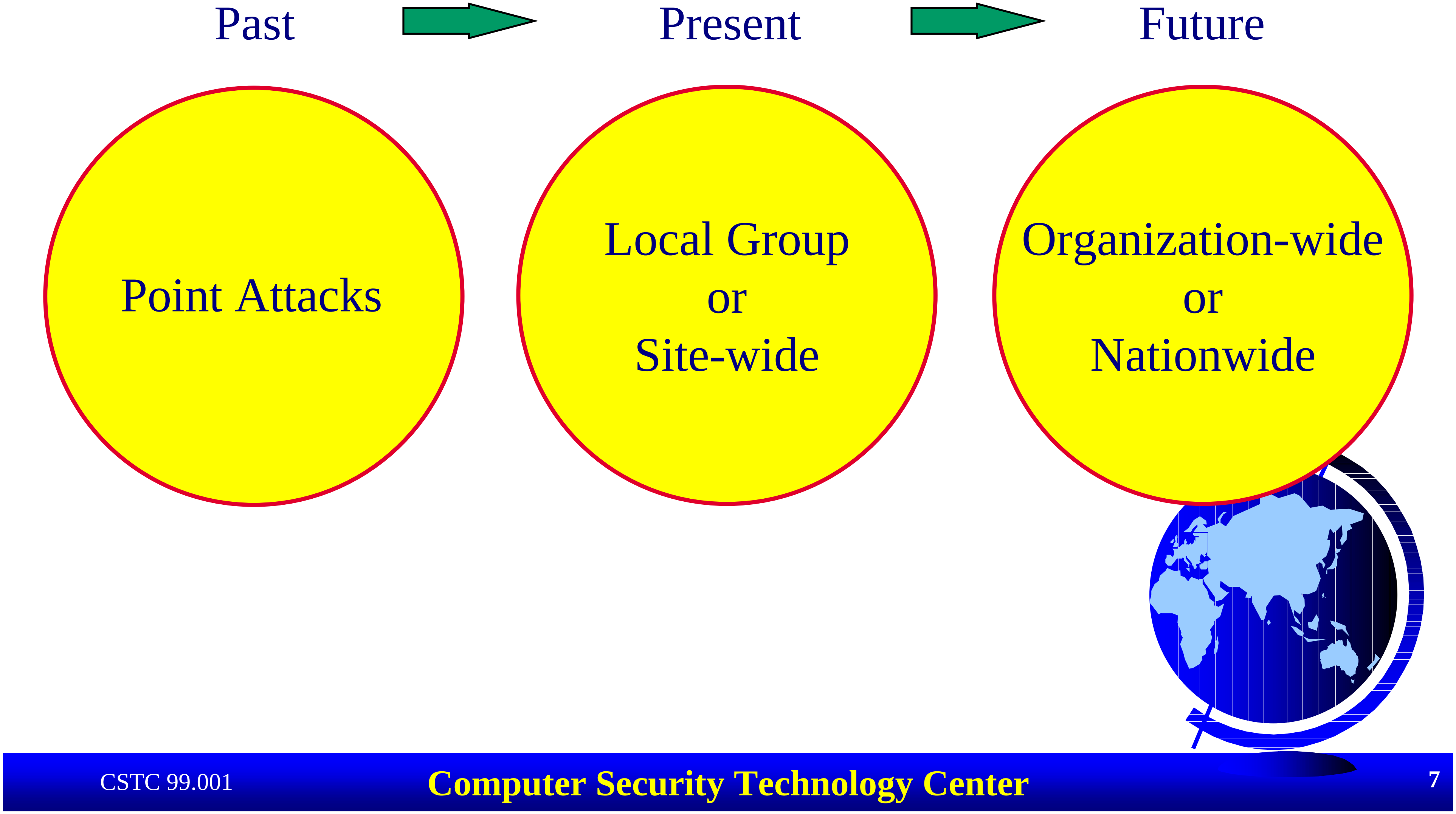
| | | |
|---|---|---|
| 1988 | 6 | |
| 1989 | 132 | |
| 1990 | 252 | |
| 1991 | 406 | |
| 1992 | 773 | |
| 1993 | 1,334 | |
| 1994 | 2,340 (more incident response teams) | |
| 1995 | 2,412 | • |
| 1996 | 2,573 | • |
| 1997 | 2,134 | • |
| 1st/2ndQ 1998 | 1,290 | |
| ***Total*** | **13,652** | |

Revised July 1998

# *FBI Computer Crime Squad*

- FBI computer crime investigations up 133% over last year
- Other sources say:
  - Extortion cases seen over last 2 decades
  - High rates of fraud in telecommunications (over 20% of all calls)
- Important note: little reporting of cyber crimes to law enforcement

# *Changing Trends*



Past → Present → Future

Point Attacks

Local Group<br>or<br>Site-wide

Organization-wide<br>or<br>Nationwide

# *Changing Trends*

- NT “Bonk” attack hit nine DOE sites
- “CERT announces widespread reports of MSCAN scans”

  --http://www.cert.org/summaries/CS-98.07.html (8/98)
- Coordinated attacks from several locations
  - Attacks distributed for stealth
  - Several individuals involved

    --SANS Digest Vol 2 Num 8 (9/98)

# *Emerging New Types of Attackers*

- Military adversaries around the world developing information warfare capabilities
  - May be responding to highly-visible US actions (AFIWC, FIWC, LIWA, etc.)
  - Considered an "asymmetrical" threat
- First known case of cyber terrorism (5/98)
  - Attack on embassies' networks by Tamil guerrillas

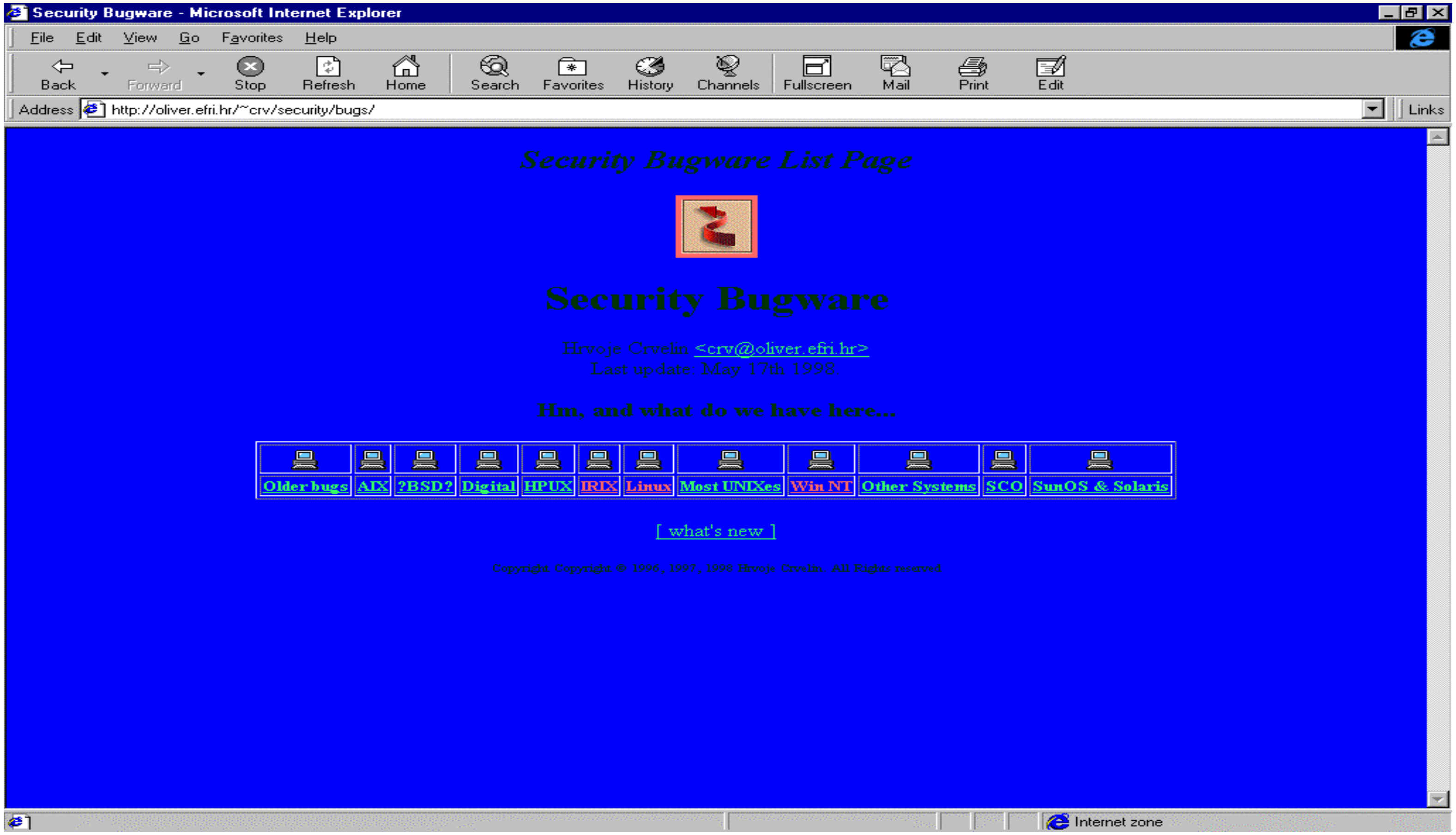
# *Attacks--How hard is it?*

- Organized crime learning high-tech methods
  - Theft of funds, money laundering, “fixing” tickets, get-out-of-jail free
- Against LLNL the major attack methods:
  - Simply “sniffing” a password off the Internet
  - Using Rootkit
  - Scanning
  - Viruses

# *How hard is it?*

- Hacking 101A: Altavista: 629 sites
  - http://www.thecodex.com/hacking.html
  - http://www.phrack.com/
- *The Happy Hacker* by Carolyn P. Meinel
- Scientific American (10/98)

# *Cracker sites*



http://oliver.efri.hr/~crv/security/bugs/

*Security Bugware List Page*

## Security Bugware

Hrvoje Crvelin <crv@oliver.efri.hr>
Last update: May 17th 1998.

**Hm, and what do we have here...**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Older bugs | AIX | ?BSD? | Digital | HPUX | IRIX | Linux | Most UNIXes | Win NT | Other Systems | SCO | SunOS & Solaris |

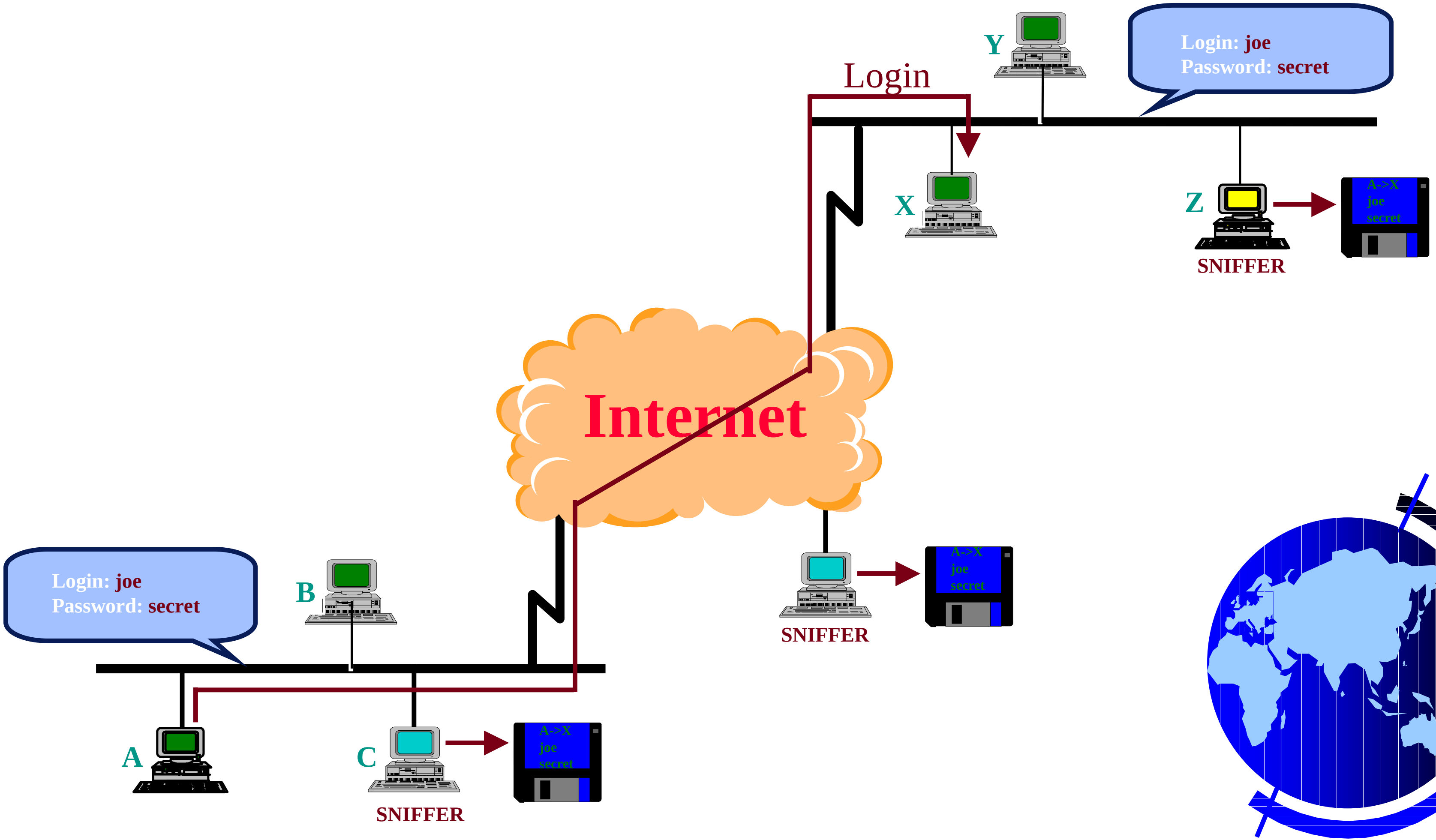
[ what's new ]

Copyright Copyright © 1996, 1997, 1998 Hrvoje Crvelin. All Rights reserved

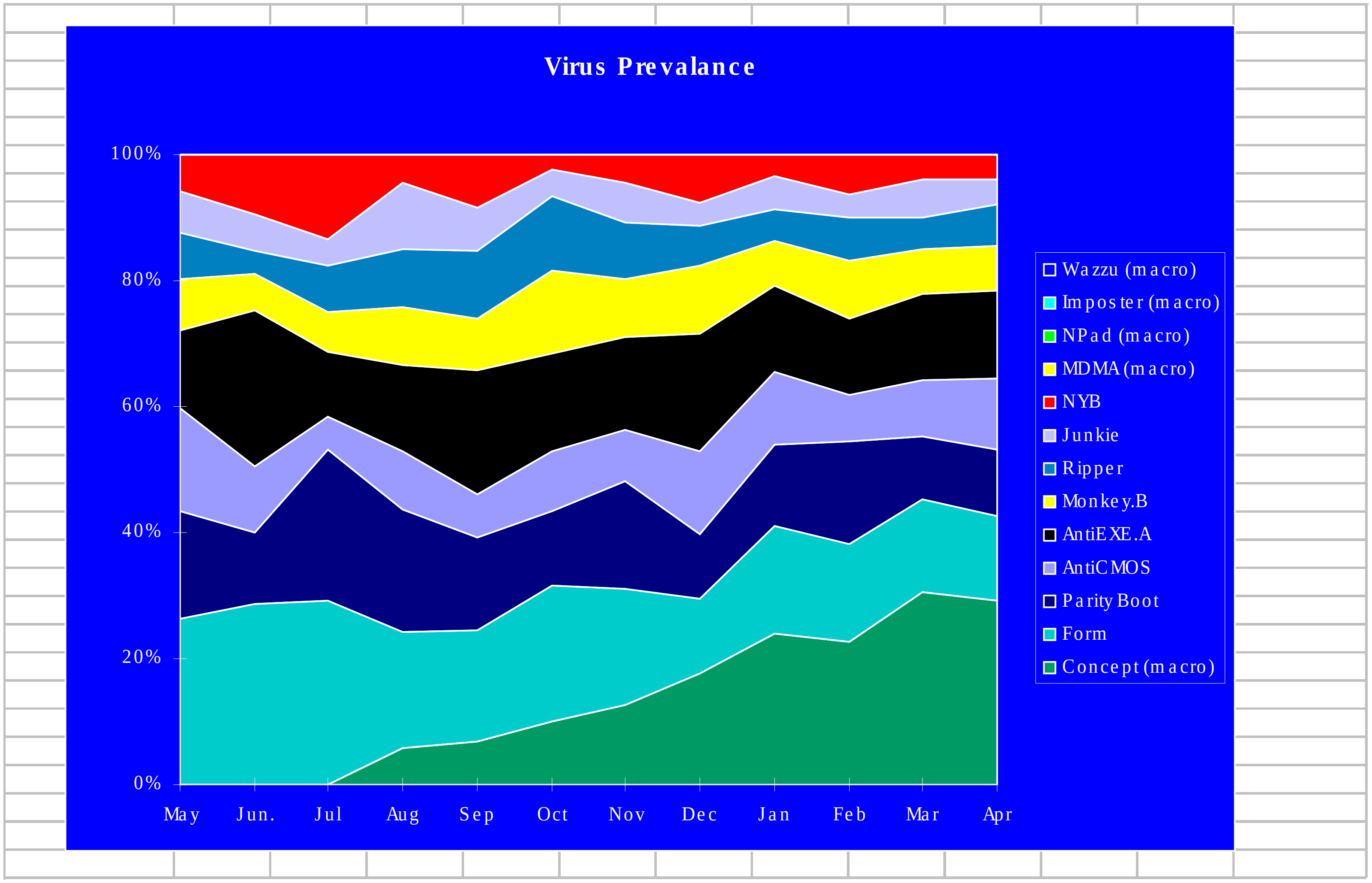
# *Attacks--How hard is it?*

- Expert hackers create sophisticated tools for everyone
  - Stealth capabilities
  - Spoofing/masquerading very easy
  - Many unpatched systems
  - Sniffers
  - Flooding (denial) attacks [hard problem] Ping ‘o Death, SYN flood

# “Sniffers” can lurk anywhere



# *Virus Prevalence*



# *Rate of Computer Viruses*

- Computer virus infection rate triples in one year
- “Macro” viruses increase 5-fold
- All this, even with $640M in anti-virus software sold
- Nearly all respondents had problems, 40% of machines infected per year

-National Computer Security Assoc. Study

http://www.relaypoint.net/~patriot/news/virus0.htm

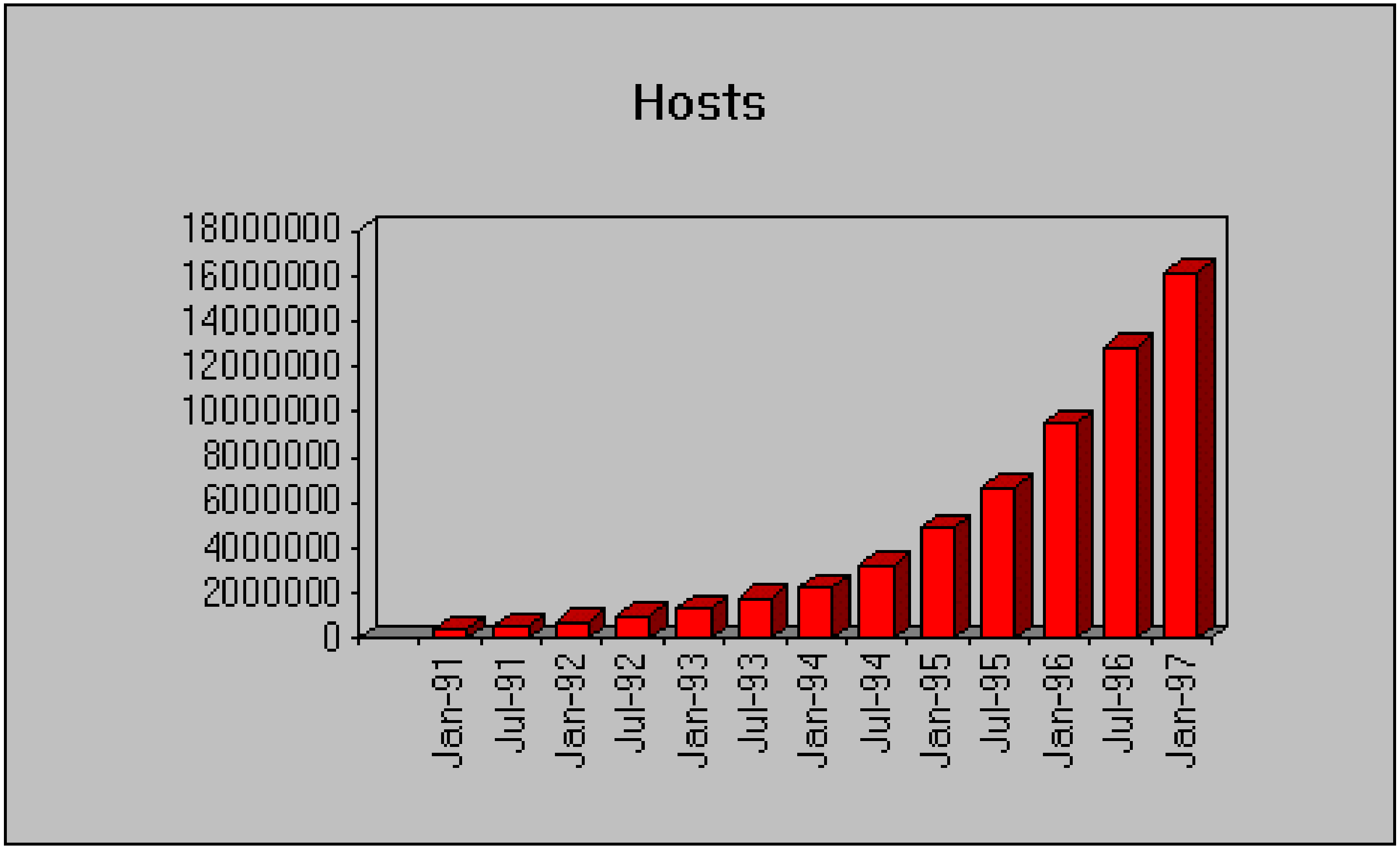
# *Attacks, cont'd*

- Web home pages have been attacked
  - US Department of Agriculture
  - Department of Justice
  - NASA (again)
  - US Department of Commerce
  - CIA
  - USAF
- 64% of companies polled had their systems attacked last year

# *Attacks, cont'd*

- From Jim Ellis, CERT/CC
  - More use of encryption by intruders (to hide their activities better)
  - Also, some tools "erase the footprints"
  - Lack of source code no longer a problem to the attackers
  - More attacks on the network infrastructure itself
- Importance of networks growing exponentially

# *Internet computer use has roughly doubled each year*



# *Lexicon of hacking:*

| | |
|---|---|
| warez | stolen software |
| phreaking | phone system attacks |
| cracking | computer/network attacks |
| newbies | new (ignorant) wannabies |
| social engin. | manipulating someone's thinking |
| anklebiters | just use tools |
| cruft | result of shoddy work |

●●●

see: *Hackers' Handbook*

# *Getting the big picture*

- Work with CIAC so we can look for organized and/or widespread attacks
  - It is especially important to consider the purpose of the systems compromised
- In turn we can warn others, DOE HQ, and the National Infrastructure Protection Center (NIPC)

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

925-422-8193
ciac@llnl.gov

NIPC

DOE sites

DOE sites

# *How to get help*

- National Infrastructure Protection Center (NIPC)
  - Chartered to help defend all of the Nation’s critical infrastructures
  - Multi-agency and private sector effort
  - “…our role is to serve as the federal government’s focal point for crisis response and investigation.” --Mike Vatis, Director
- Forum for Incident Response and Security Teams (FIRST)
- cstc@llnl.gov
- Private firms (e.g., IBM, SAIC, Booz-Allen, etc.)
- cert@cert.org

# How to help IH folks:

- Collect as much as is tolerable
  - Firewall and router accept/deny logs: *a single choke point*
  - Operating system audit logs
  - Network packet logs: *turn packet sniffers on the hackers*
    - Capture connection records and packet data records
  - Application audit
    - Example: UNIX TCP Wrapper controls, monitors, and reacts to network connections
    - Example: Oracle database authentication failures
  - Defense-in-depth: *monitor intruders at multiple levels/locations*
- Automate reduction
  - Real-time is preferred over batch or random checks
  - Example: UNIX Watcher, TkLogger, Logcheck

# *Prevention Techniques*

- Firewalls-almost universal in top companies
- Monitoring tools (some can react also)
- Strong authentication (one-time passwords) [s/key, smartcards, DCE]
- Scanners (e.g., ISS, SATAN, etc.)
- Other electronic assessments (e.g., SPI, COPS, Tiger)
- Anti-virus tools

# *Vendors*

- Some vendors now very responsive to problems with their systems
- Many still shipping systems wide open (e.g., no passwords, well-known defaults)
- Systems not checked--old errors
- Growing commercial activity--consolidation of the field

# *Good security sites*

- http://www.cs.purdue.edu/coast/coast.html
- http://niim.bus.utexas.edu/index.htm

- Bottom line: Partial solutions are available today!

# *Questions?*

- To obtain a copy:
  - Doug Mansur<br>
    Lawrence Livermore National Laboratory
    P.O. Box 808, L-303
    Livermore, CA 94550
    mansur@llnl.gov
    925-422-0896
- More info:
  - cstc@llnl.gov, ciac@llnl.gov, http://ciac.llnl.gov/cstc, http://ciac.llnl.gov, http://doe-is.llnl.gov